

13th ICCRTS: C2 for Complex Endeavors

**An Automated Information Asset Tracking Methodology to Enable
Timely Cyber Incident Mission Impact Assessment**

Topic 1 - C2 Concepts, Theory, and Policy
Topic 9 – Collaborative Technologies for Network Centric Operations
Topic 4 – Cognitive and Social Issues

Michael R. Grimaila¹, Robert F. Mills¹, and Larry W. Fortson²

¹Air Force Institute of Technology; Wright-Patterson AFB, OH USA

²Air Force Research Laboratory; Wright-Patterson AFB, OH USA

Point of Contact:
Michael R. Grimaila
Center for Cyberspace Research
Air Force Institute of Technology
AFIT/ENV
Wright-Patterson AFB, OH 45433-7765
937-255-3636 x4800 (DSN 785)
Michael.Grimaila@afit.edu

An Automated Information Asset Tracking Methodology to Enable Timely Cyber Incident Mission Impact Assessment*

Michael R. Grimaila¹, Robert F. Mills¹, and Larry W. Fortson²

¹Air Force Institute of Technology; Wright-Patterson AFB, OH USA

²Air Force Research Laboratory; Wright-Patterson AFB, OH USA

Abstract. The use of information technologies to enhance Command and Control (C2) processes has yielded enormous benefits in military operations. Commanders are able to make higher quality decisions by accessing multiple information resources; obtaining frequent updates; and by correlation between resources to reduce battlespace uncertainty. However, the dependence upon information technology creates significant operational risk that is often overlooked and is frequently underestimated. Risk management is the accepted process used to identify, value, and protect critical assets commensurate with their value. Risk analysis, the first step of the risk management process, requires the identification and documentation of organizational resources and determination of their criticality. While risk analysis is conceptually easy to understand, in practice it is difficult to conduct due to the dynamic nature of organizations, the temporal nature of operations, and the inherent subjectivity associated with valuation. In this paper, we propose a scalable, self-documenting, distributed information asset tracking methodology that identifies information dependencies, does not incur significant overhead, and prevents an adversary gaining knowledge from intercepted communications. The method is made feasible via the wide-spread deployment of Host-Based System Security software agents by JTF-GNO and can significantly enhance cyber damage assessment timeliness and accuracy and enables mission impact assessment.

Keywords: situational awareness, cyber damage assessment, information architecture

1 Introduction

Information is a critical asset to all modern organizations, but especially so for the military which uses information to conduct all aspects of its operations [1]. Information is collected, processed, analyzed, distributed, and aggregated to support situational awareness, operations planning, intelligence, and command decision making [2]. The need to incorporate information technology to reduce response time and to increase decision quality is a direct consequence of the nature of modern warfare which is technology enhanced, fast-paced, with high-intensity conflicts [3]. Commanders are tasked with making critical decisions in short time frames based upon limited information. Since the quality, conciseness, and timeliness of the information used in the decision making process dramatically impacts the quality of command decisions; the recognition,

* This work was supported by a research grant from the Air Force Research Laboratory (F4FBBA7144J001).

quantification, and documentation of these information dependencies is essential to provide accurate and timely damage and mission impact assessment [4][5][6]. Recently amended military joint guidance requires commanders to ensure operational impact assessment is accomplished following a cyber incident. In fact, we believe that commanders must be kept aware of how a cyber incident affects, or may potentially affect, their mission operations from the instant it is discovered until the time it is remediated. Unfortunately, our existing approach to impact assessment does not provide this knowledge in an accurate or timely manner.

Military operations differ from non-military operations in many ways, but especially due to their dynamic nature and the criticality of consequences resulting from degraded decision making. Despite this difference, we can borrow from the methods used in securing non-military organizations to improve our abilities to provide accurate and timely damage assessment. Pipkin recognizes the importance of identifying critical information in his five phase process for managing organizational information security: Inspection, Protection, Detection, Reaction, and Reflection [7]. The Inspection phase requires the identification, valuation, and assignment of ownership of information assets and information dependencies critical to the organization before and incident occurs; the Protection phase requires the assignment of the control measures to protect critical information assets commensurate with their value; the Detection phase requires the development of robust detection capabilities to insure that any breach of the organization is detected in a timely manner; the Reaction phase requires that the organization has developed the resources and capabilities to quickly respond, contain, investigate, and remediate breaches; and the Reflection phase requires effective post-incident documentation, reporting, and accountability to assure institutional learning. Pipkin asserts that neglecting any one of the five phases can expose the organization to excessive losses when they inevitably experience an information incident. Unfortunately, we believe the Department of Defense (DoD) has neglected to properly standardize the first and last phases. While we have developed significant expertise and capabilities in the Protection, Detection, and Reaction phases; we have failed to adequately identify, value, track, explicitly document, and report our cyber resources (Inspection) and also to document, report, and hold organizational units accountable for lapses in information security (Reflection). As a result, we artificially constrain ourselves which seriously limits the timeliness and accuracy of the damage assessment and makes dominate battlespace knowledge in cyberspace virtually impossible.

In this paper, we discuss the importance of accurate and timely damage assessment in military operations; motivate the need for a change in existing assessment methodologies; discuss viewing information as an asset; and propose a scalable, self-documenting, distributed information asset tracking methodology that identifies information dependencies, does not incur significant overhead, and prevents an adversary gaining knowledge from intercepted communications. The proposed method is made feasible by the wide-spread deployment of Host-Based System Security (HBSS) software agents by JTF-GNO; will significantly enhance cyber damage assessment timeliness and accuracy by requiring organizations to identify and value their dependencies on information; and enable mission impact assessment by providing the foundation needed to build an automated, predictive situational awareness tool.

2 The Importance of Damage Assessment

Accurate and timely damage assessment has been a critical determinate in the quality of command and control decision making since the dawn of organized warfare [8]. The need to quickly assess the impact of offensive operations against the enemy is critical because it enables the commander to efficiently plan future operations and to deploy assets in support of the stated mission objectives. Similarly, from a defensive perspective the commander must be fully aware of the current status of all of its support elements. Admiral William A. Owens captured this idea in his model for understanding the technology enhanced battlespace where ideally a commander would have Dominant Battlespace Knowledge (the ability to see the whole battlespace in near-real time for situational awareness), Immediate/Complete Battle Assessment (the ability to have immediate feedback about his troops' actions), and Near-Perfect Mission Assignment (the ability to command his troops with as little latency as possible) [9]. While Owens model was focused on the use of technology in the physical battlespace, it takes on enhanced meaning when you consider how cyberspace is embedded into all aspects of real world operations. The loss of a cyber resource may impede or inhibit the ability to conduct real world operations.

The need for improved damage assessment in the cyber domain is not a recent development. In 1995, the Rand Corporation conducted a series of exercises known as "The Day After" that were designed to simulate information warfare attacks and to measure the ability of organizations to respond to the attacks [10]. The results of the exercise identified numerous critical issues that must be addressed to improve the DoD response to cyber attacks. Among these was the realization that the application of traditional physical damage assessment methodologies failed to produce meaningful defensive damage assessment following an information compromise. The report cited the need for "mandatory reporting of attacks to help better identify and communicate vulnerabilities and needed corrective actions" and "damage assessments to reestablish the integrity of the information system compromised by an attacker." Despite these critical findings, more than a decade later we still do not have a standardized DoD wide cyber damage assessment process in place [6,11,12]. This significantly hinders our ability to develop an enterprise wide view of the impact resulting from a cyber incident.

3 The Need for Mission Impact Assessment

Damage assessment and mission impact assessment must not be viewed as the same thing. Existing methods for quantifying damage tend to use easy to assess technical measures (such as the loss of availability and man hours required to remediate) and are primarily focused upon rapid system restoration [6,12,13]. While this information is an important, it does provide an understanding to the commander of how their organizational mission is impacted by the incident. Arvidsson identified that cyber damage is a consequence of "an attack which affects the normal operation of the targeted system or service" and that impact describes the result of the damage caused by the attack "expressed in terms of user community" [14]. Damage is "a reduction in value resulting from some external action" [15]. Damage assessment is concerned with determining damage in terms of value loss of the affected cyber resource resulting from an incident. In contrast, mission impact assessment is an evaluation of how the damage impairs, or potentially can impair, the affected organization(s) mission operations.

Mission impact assessment is an essential requirement to enable Situational Awareness (SA). Endsley's Level 2 SA requires that there is a detailed understanding of the significance of the sensed elements in light of the operator's goals [16]. In cyberspace, the commander must have an understanding of the impact, and potential impact, of a cyber incident. Without a documented understanding of how the information contained on a system supports the organizational mission, any efforts at attaining Level 2 SA will be seriously handicapped. Taddaa et al. also recognized the need for quantifying the importance of mapping in the Level 3 of their cyber SA model [17].

Security risk management is the process most often used by organizations to identify risks and determine optimal protection strategies when constrained to a limited security budget [18]. Organizations typically employ a risk management strategy that assesses threats, vulnerabilities, potential losses in order to select control measures (e.g., people, processes, technology) to mitigate risks in a cost effective manner. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 "Risk Management for Information Technology Systems," identifies that risk management is composed of three processes: risk assessment, risk mitigation, and evaluation/assessment [19]. Risk analysis, the first step of the risk management process, requires the identification and documentation of critical organizational resources among all resources that are used to support the organizational mission. Determining the criticality is not trivial; it requires an estimation of the value the resource provides to the organization based upon how it supports the organizations strategic objectives [20,21]. The scale and complexity of the organization; interdependencies between resources; and the dynamic nature of resource utilization greatly complicates value determination. However, an accurate estimation of the resource value is essential as it directly impacts the quality of the decisions made during risk management [19]. The valuation, in conjunction with an estimation of threats, vulnerabilities, and the likelihood (per unit time) of their intersection, is used to determine the potential loss against a resource given the state of the organizational security capability. Collectively, this information provides the ability to "rack and stack" and address risks by risk avoidance, transference, mitigation, or acceptance commensurate with the value of the resource.

Unfortunately, the DoD does not currently require its component organizations to conduct a standardized, formal, well-documented risk management of its cyber resources with a focus of real-time impact assessment [6]. Instead, existing guidance mandates compliance with the DIACAP process, which was designed to assure the operational security capabilities and security controls of a cyber resource, not to provide damage assessment information [22,23]. As a result, the information that would be collected during the risk assessment phase is not available, preventing the accurate and timely estimation of damage and mission impact resulting from a cyber incident.

What are the consequences of accepting the status quo? Each day, we are the target of multiple attacks by adversarial forces in cyberspace. Even if we are successful at detecting, containing, and remediating a cyber incident in a timely manner, the failure to immediately assess the damage and report the mission impact to commanders may result in other unforeseen higher order effects that may not be immediately apparent at the time of the incident. Consider the following hypothetical scenario.

In this scenario, a deployed military organization is conducting an active military operation on foreign soil. One element of the operation requires the periodic delivery of supplies between facilities located in different parts of the country via ground vehicles. The commander of the unit uses a logistics management program that stores the convoy routes and schedules in a database. A system administrator needs to upgrade the server containing the database, so he temporarily relocates it to an existing database server located in another organizational unit without formally documenting the change. In the meantime, access to our network is provided to a coalition partner to facilitate information sharing on an unrelated operation. Unfortunately, the coalition partner does not enforce stringent access control policies and as a result, an adversary breaches the coalition partner's system and subsequently breaches the database server containing convoy routes and schedules. The incident is detected by Incident Response Team (IRT) who terminates the adversary's access to the database and begins to investigate and remediate the breach. The problem is that there is no explicit documentation which identifies all of the entities who depend upon information stored in the database or how their mission would be impacted by a breach. Before the IRT can comb through the log files and notify the affected parties, a convoy listed in the database is ambushed resulting in a significant loss of life and resources. While the scenario presented is hypothetical, it demonstrates the dire consequences that can result from failing to properly track the status of critical information assets.

4 Information is the Most Important Asset in Cyberspace

Existing cyber defense strategies tend to focus on the infrastructure assets rather than the information resources that are being accessed [6, 12]. This approach is inherently limited in its ability to identify the risks to the resources the organization intends to protect [24]. It substitutes the value of the resource being used with that of the infrastructure elements. The assumption that technology is an equitable substitute for information is a dangerous assumption and follows a proven path of failure [25]. While we agree that infrastructure elements are important, their value is dominated by the value of the information stored, retrieved, processed, and transported through the infrastructure. Further, without the context of the use of by the end user(s), data has no inherent value [26]. Information is the center of gravity for operations because it holds relevance and value as knowledge to decision makers in the organization [27,28]. Human utility organizes and aggregates data into usable groupings of contextual relationships that endow the data with "relevance and purpose" [25]. Through interpretation, data becomes information and is inherently associated with meaning [26]. For these reasons, we propose that information, not data, should be the focus when developing methods to improve cyber damage and mission impact assessment.

Previous research recognized the importance of information and proposed a conceptual framework for improving cyber damage assessment [6]. Figure 1 below shows a timeline of the framework. Of particular importance are the pre-incident activities which require the proper identification and value assessment of information assets which are mapped to mission criticality.

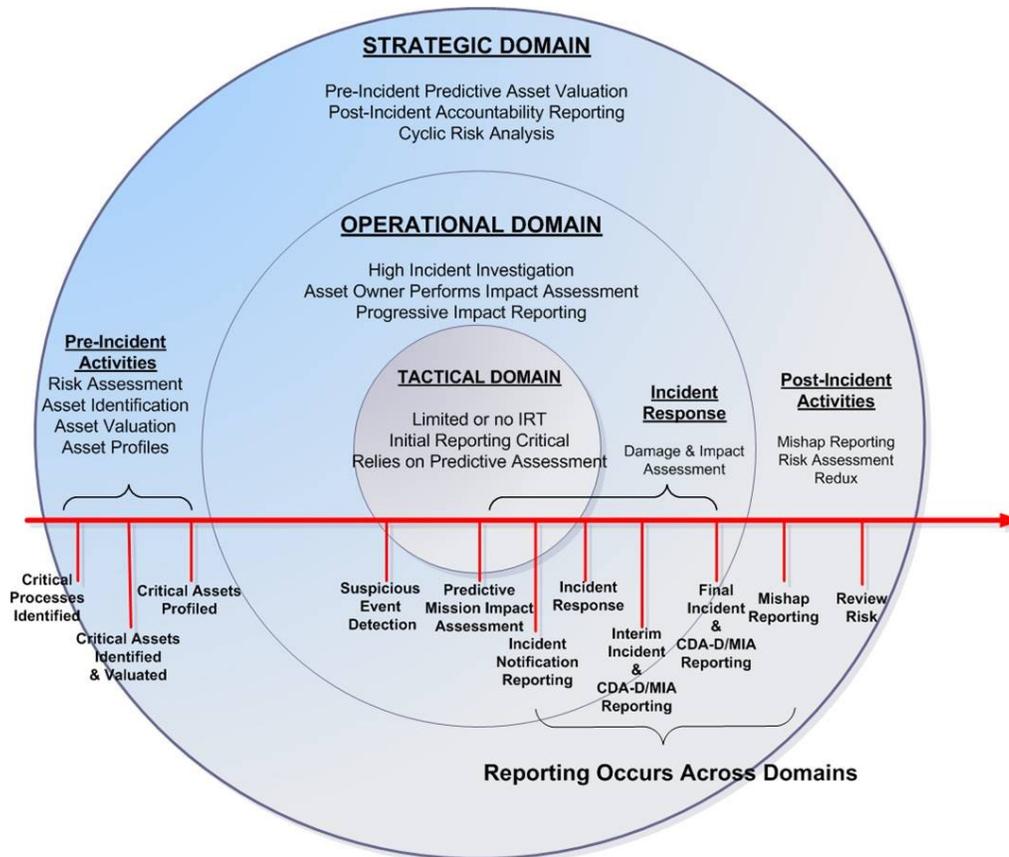


Figure 1: Defensive Cyber Damage and Mission Impact Assessment Timeline

The identification and valuation of information dependencies must occur before an incident occurs. Identification of an information dependency inherently implies there is a supplier (source) of the information and a consumer (sink) of the information. In some cases, both the information supplier and consumer may be within the same organization, in others they may be in different organizations. Regardless, each organization must first identify, document, and value its information dependencies. This can be accomplished through an information asset-focused risk assessment or using other similar information asset profiling techniques [19, 29, 30].

Information dependencies must be valued and a threshold selected to determine if the asset is “critical.” Assigning security classifications allows for the logical grouping of resources to assign general security levels so that information of a particular security level will always get a prescribed minimum level of security based upon the organizations policies. The military does this with classifications and categories and involves determining the value of the information with respect to the impact on national security. There are varying degrees of importance and sensitivity to information for a corporation, the classification system should be used, “to ensure that the information receives the appropriate level of protection” [7]. Factors such as; sensitivity of the information, consequences of disclosure, legal and contractual obligations and penalties, standards and guidelines, and the information lifecycle should be taken into account with respect to the information’s overall confidentiality, (impact from disclosure), availability, (urgency/ loss

of not having the information) and integrity (knowing and trusting that the information is unaltered from its intended state).

Determining the value of an information asset is a complex task, due to its inherent intangible qualities [31]. While many existing valuation models rely on tangible economic metrics when conducting an information value appraisal, the intangible value of information in a military context often far exceeds its tangible economic value. The DoD possesses a distinct advantage in determining a baseline for the value of its information assets because information is assigned a classification through its uniform system for classifying, safeguarding, and declassifying national security information [32]. However, this only provides a coarse “first cut” for determining the value of information in the context of how it may impact national security and not the organizational mission.

We emphasize that any valuation of information must be from the perspective of the organization making the valuation. This makes it difficult to aggregate information value across organizations without first developing a canonical, enterprise wide information valuation scheme. Information value determination is difficult as there are both tangible and intangible value components that must be accounted for; the value of information changes over time; and the operational need for information changes over time. This is especially difficult in military organizations where the missions are dynamic and ever changing. Despite these challenges, an estimation of information value made by the end users of the information is far superior to an estimation made by someone unaware of the utility of the information. One proposed value scheme used to assess information criticality in support of the organizational mission is shown in Figure 2 [6].

1 Little Mission Utility Non-Critical	2 Weak Mission Utility Non-Critical	3 Some Mission Utility Non-Critical	4 Strong Mission Utility Important	5 Highest Mission Utility Important
Lowest Value	Low Value	Moderate Value	High Value	Critical Value

Figure 2: A Mission Value Estimation Scale

Information dependencies and their valuation must be documented in a standard, clear, unambiguous manner. Documentation is required to enforce accountability, to insure that the estimation of the value can be refined over time, to provide transparency, to reduce the time required to understand the impact of the loss of a resource, and to reduce the excessive variances in loss estimation. In our research, we have found that organizations neglect to create and maintain this important documentation for a variety of reasons: difficulties in obtaining the required information from knowledgeable individuals; the lack of resources required to collect, record, and maintain the information; fear of embarrassment if an incident occurs which hinders their operations; and most importantly the fear that if this information is not properly secured it may be used as a targeting map by an adversary. We are convinced that with the proper resources we can overcome these barriers and supply meaningful mission impact assessment, enable accurate predictive situational awareness, and develop a timely understanding of possible adversarial intent during a cyber incident. If we accept the idea that information is an asset, we

must develop a standardized scheme for identifying, valuing, tracking, documenting, and reporting information assets. In this paper, we propose an information architecture and methodology to automate the tracking of information assets to enable the timely and accurate estimation of the impact, both in terms of damage and mission impact, resulting from a cyber incident.

5 Cyber Incident Mission Impact Assessment (CIMIA)

In this section, we examine shortcomings in existing guidance and provide a brief summary of our Cyber Incident Mission Impact Assessment (CIMIA) project as motivation for the proposed information asset tagging methodology. The purpose of the project is to develop an operational methodology that organizations can use to assist in the identification, valuation, documentation, and reporting of critical information asset dependencies in order to provide near real time cyber damage and mission impact assessment. The project is a continuation of the work started in understanding shortcomings in defensive cyber damage assessment [4,5,6].

5.1 Existing Guidance

NIST SP 800-30 states, “the principal goal of an organization’s risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets” [19]. Risk management should not be treated primarily as a technical function carried out by the IT experts who maintain and operate the system, but as an essential management function of the organization. This is integral point is at the core of the problem with existing guidance and can not be over looked. AFI33-138 “Enterprise Network Operations Notification and Tracking” states that the MAJCOM senior communicator will: (when delegated) act as the Designated Approving Authority (DAA), to approve or disapprove system connections to the network [33]. At the base level, the Wing Information Assurance (IA) flight is tasked with providing training, recommendations, and assistance to all tenant organizations in regards to information assurance issues. According to AFI 33-202V1 “Network and Computer Security” the Wing IA flight is the focal point to track all wing and tenant unit compliance with certification and accreditation (C&A) requirements [34]. As well, for any suspected incidents of contaminated systems, the Wing IA flight is to ensure remediation is implemented. AFI 33-138 identifies what is to be reported and what timelines to do so as shown below in Table 1 [33].

Table 1: AFI 33-138, Security Incident Reporting Action Matrix

If the originator / recipient of the IR is	then take the indicated Actions	and the Primary Recipient will be	and Informational Recipients will be
End User	1	WM	N/A
WM	2, 8	NCC	ISSO and FSA
FSA	2, 8	NCC	ISSO/ISSM
ISSO	2, 8	NCC	ISSM and Wing IA Office
ISSM	2, 8	NCC	Wing IA Office and DAA

13th ICCRTS: C2 for Complex Endeavors

NCC	3, 8	NOSC	Wing/FOA/DRU IA Office and DAA
NOSC	4 - 8	AFNOSC	MAJCOM IA Office and MAJCOM DAA
Actions			
1	Upon detection of an incident, end users will immediately notify their assigned WM and provide information to assist the WM making required notifications and in filling out an IR. If the WM is unavailable, end users will immediately notify the next computer security professional in the chain of command (i.e. FSA, NCC, NOSC, ISSO, ISSM, etc.).		
2	Upon detection or notification of an incident, the WM, FSA, ISSO, or ISSM will notify their servicing NCC. After notifying the NCC, the WM, FSA, ISSO, or ISSM will prepare and transmit an IR to the servicing NCC. If there is no servicing NCC, send the IR directly to the parent NOSC.		
3	Upon detection or notification of an incident, notify the parent NOSC. After notifying the NOSC, prepare and send an IR to their parent NOSC.		
4	Upon detection or notification of an incident, contact the AFNOSC for assessment of the incident and assignment of an IRID (upon validation).		
5	After making initial contact with the AFNOSC, follow-up by submitting an initial IR and generate a UEC4N to track the event.		
6	Submit an update IR every 7 days until all actions required to resolve the incident are complete.		
7	Submit a final IR within 24 hours of all action related to the incident being completed.		
8	Send an informational copy of all IRs to the Informational Recipients indicated		

With the senior MAJCOM communicator acting as the sole approval authority for base systems connecting to the MAJCOM enterprise, and the wing IA flight tasked with ensuring the remediation actions of information system security incidents, it would seem that, “the IT experts who operate and manage the IT system,” are exactly the ones that are handling the risk management of the Air Force networks. Not once in the incident reporting action matrix is an operations commander notified of a potential mission impairment due to the detection of an incident involving the confidentiality, availability, integrity and accountability of their information system.

The architecture of CIMIA was designed to rectify this problem and provide immediate utility to information providers and information consumers. Information providers need to know who is dependent upon their information resources so that the Incident Response Team (IRT) can notify these downstream consumers in a timely fashion. Further, knowledge of who is dependent upon your information resources can be used to justify resources or provide a means to “charge” organizations for use of your resources. Information consumers are required to document and value their dependencies. When an incident occurs that impacts one or more of the consuming organizations critical cyber dependencies, information about the mission impact and potential mission impact is immediately available to the commander and to the IRT which is charged with reporting impact. Figure 3 shows how the incident reporting process can be enhanced through identification and documentation of critical information assets to facilitate damage and mission impact assessment [6].

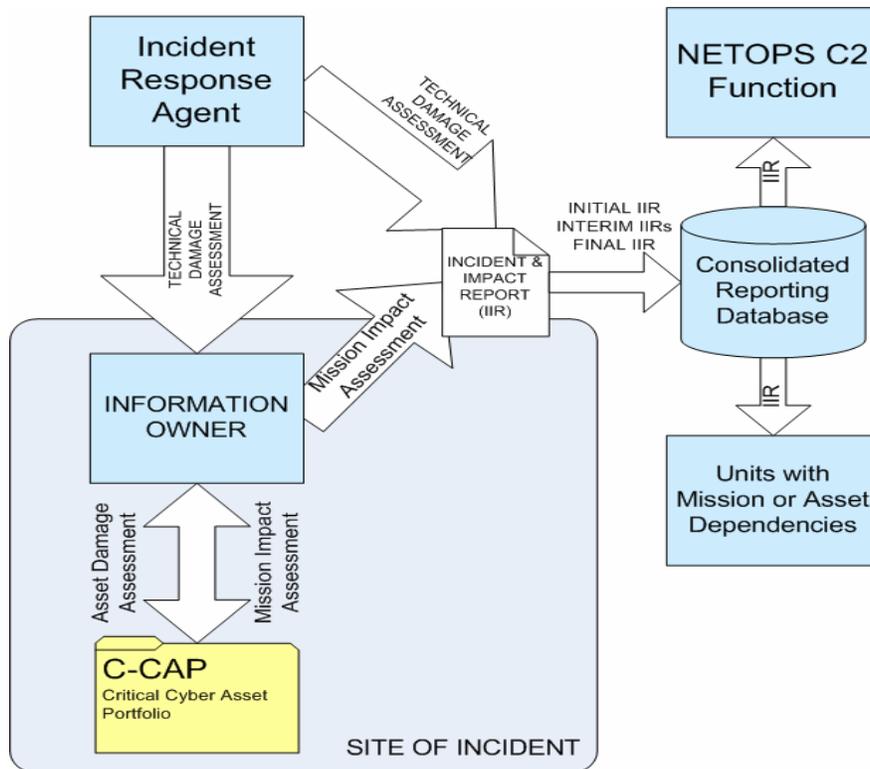


Figure 3: CIMIA Incident Reporting Process

When a cyber incident occurs, the IRT is dispatched to investigation and help in the remediation process. The IRT team will work with the organization at the site of the incident to determine the technical damage that has occurred as a result of the incident. In the CIMIA process, each organization is responsible for creating and maintaining a Critical Cyber Asset Profile (C-CAP). The C-CAP contains a list of all critical information dependencies that the organization possesses along with a quantification of the value that the information provides to the organization. The C-CAP is essential to improving the timeliness and accuracy of damage and mission impact assessment. When a cyber incident occurs, all organizations that are dependent upon the impacted cyber resource can immediately estimate the impact. Mission impact estimation can be provided to the commander from the moment a cyber incident is detected until it is remediated. As the IRT investigates, the information collected will help refine the impact estimation from a pessimistic, worst case estimation to the actual impact only determined after the investigation has been completed and remediated. Figure 4 shows an example of how mission impact assessment can be estimated from discovery through remediation.

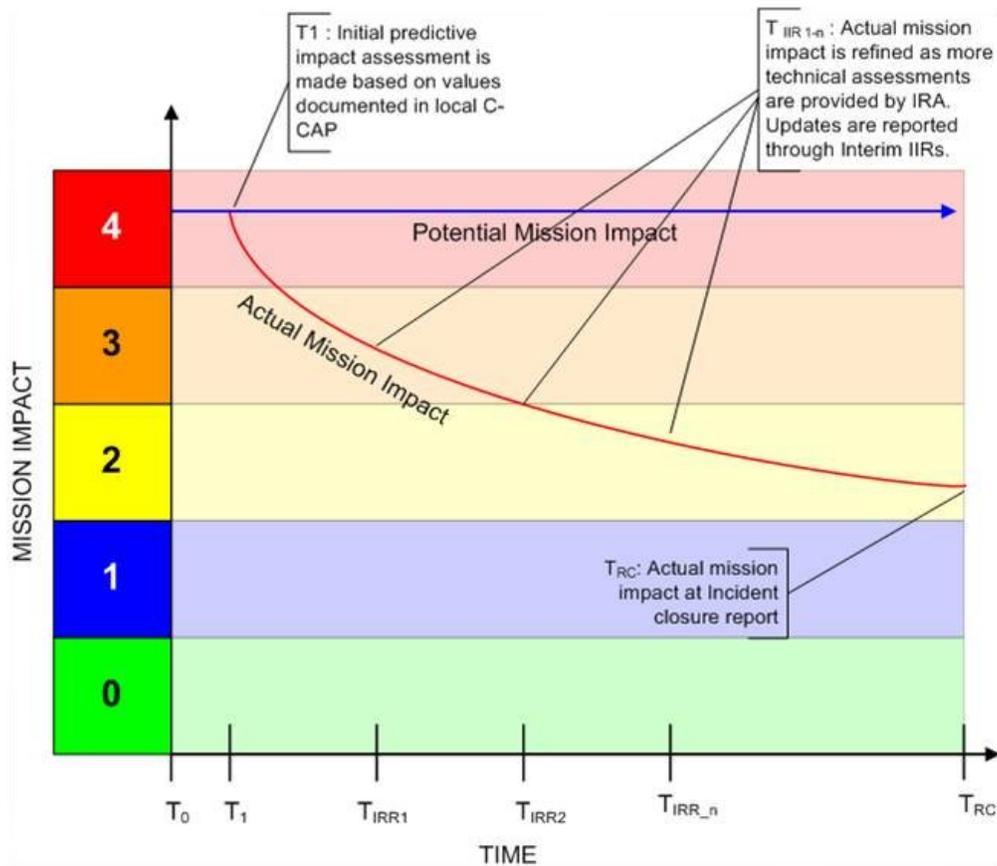


Figure 4: CIMIA Impact Estimation as a Function of Time

The CIMIA system should allow for the collaboration of the confluence of raw data available and correlate it to the consumer's particular mission in time and place relevant to the consumer. The agent will have to allow for the user to input their respective mission and the information's relevance to that mission in a secure manner. Identification of mission critical information and its valuation would have to be secured at the highest level of that particular mission's classification. Through an auto discovery method, most information devices on any network can be found and quickly loaded to a standard database. This is common practice with tools like REMEDY, and HP OPENVIEW. Configuration management practices across DoD utilize similar applications to facilitate change management. These tools should be standardized across the DoD and a standard database with a common data collection schema utilized to facilitate data-mining capabilities of enhanced decision support systems such as CIMIA.

For CIMIA to correctly correlate information assets and the users dependencies upon all of the different informational process flows within the organizational business processes, it will have to incorporate an automated mechanism for collecting where and how the user gathers information. This mechanism will have to collect information on file and server access, http requests, and common electronic mail exchanges. For CIMIA to properly correlate mission criticality there must be a way to identify all consumers of an information resource and to aggregate each consuming organizations valuation.

6 An Automated Information Asset Tracking Methodology

In this section, we introduce an information asset tracking methodology which is the foundational element in the CIMIA process. It provides the capability to automate the identification and documentation of information dependencies; securely document the valuation of information asset dependencies by information consuming organizations; track and prioritize information as it travels from source to sink through infrastructure elements; and allows information providers the capability to deterministically identify all those who depend upon their information resources.

As we have discussed, a documented risk assessment is essential to provide the information necessary for timely mission impact assessment. Unfortunately, this is a labor intensive and time consuming task with little possibility of being conducted in an environment where force reductions are underway and existing personnel are already task saturated. Since organizations tend to be dynamic entities, automation is necessary to force updates to the assessment as the organizations information dependencies change. Although automation of the identification of information dependencies are possible, the identification of the mission processes that are supported by the information dependency and the valuation of information dependency must be conducted by the human being who consumes (uses) the information. The CIMIA approach requires that information consumers 1) explicitly link each information dependency to the mission process(es) that it supports, and 2) explicitly assign a value to the criticality of each information dependency.

The information collected from each information consumer within an organizational will be collected into an organizational database that serves as the organizations Critical Cyber Asset Profile (C-CAP). The C-CAP provides the information required to provide near real time damage and mission impact assessment in response when a cyber incident occurs. The C-CAPs from each organization are transmitted in a secure channel to an enterprise wide central authority who can determine all of the information dependencies and their valuation, calculates aggregate information resource valuations, and can identify and notify all downstream consumers when a cyber incident occurs.

6.1 Preliminary Definitions

An information *source* (provider) is defined as any network node that provides an information resource to one or more information *sinks* (consumers). Each information resource is uniquely defined by a triple containing the IP address, port number, and resource number (<IP address, port number, resource number>). A triple is required to uniquely identify the resource because multiple information resources may be accessed from the same IP address and port number pair. For example, a single instance of an SQL database may allow access to multiple databases based upon the connect command issued by the consumer. Each information resource is uniquely identified by an encrypted tag that is periodically inserted into the requested information.

An information *sink* (consumer) is defined as any network node that requests and receives an information resource from an information *source* (provider). An information sink is defined by the triple containing the IP address, port number, and consumer number (<IP address, port number, consumer number>). The IP address and port number pair alone is not sufficient to uniquely define the consumer of the information resource. Since multiple operators may use the same system, the consumer number is provided to uniquely identify the information consumer.

6.2 Information Asset Tags

For CIMIA to properly correlate mission criticality there must be a way to identify all consumers of an information resource. This is accomplished through the insertion of a multiple byte tag at the source which uniquely defines an information resource. The first time an information consumer accesses an information resource, and periodically thereafter, the tag is inserted into the data stream as shown in Figure 5.

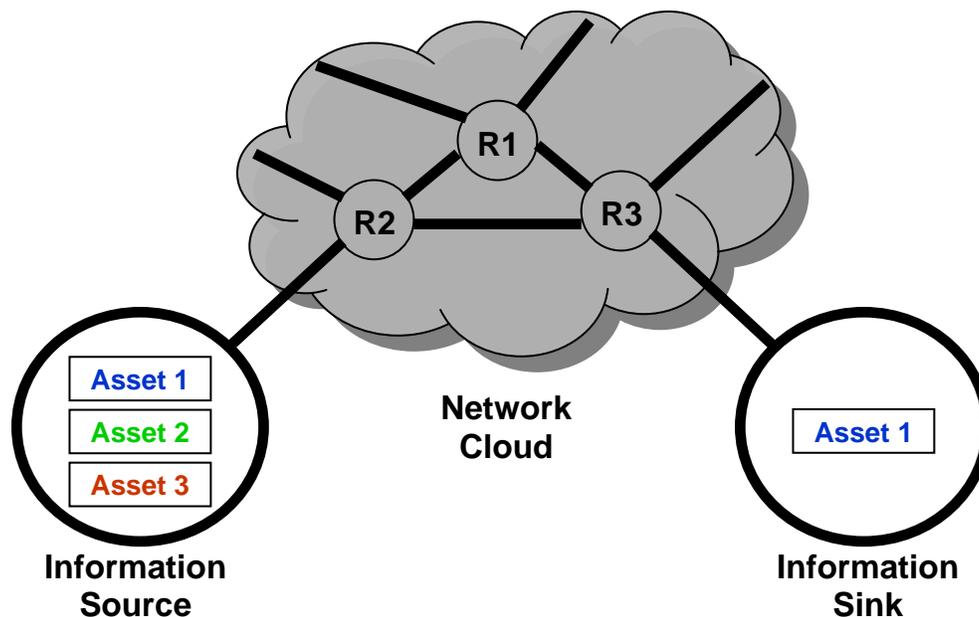


Figure 5: CIMIA Information Source Sink Architecture

In this case, information Asset 1 is being requested from the information source (provider) by the information sink (consumer). The information source (provider) responds to the request and inserts an encrypted tag into the information which is transported through router R2, to router R3, and then to the requesting information sink (consumer). The tag must not contain information (such as criticality or priority) that could be exploited by an adversary who was eavesdropping on a network communication. Instead, the tag is an encrypted pointer into a multilevel security database (e.g., Secure Oracle OLS) loaded on a trusted operating system and can only be accessed via a separate high side network (e.g., SIPRNET or higher security

network) maintained by a central authority (e.g., JTF-GNO). Access to the database is restricted only authorized individuals with a need to know the information contained within the database.

When an organization places an information resource on the network, they will request a tag from a central authority. Each tag issued is unique and corresponds to an entry in the high side database that contains information about the creator, owner, producer, distributor, pedigree, age, composite elements, security classification, security compartment(s), rated criticality, and derived criticality of the information resource as well as other relevant properties of the information resource. The organization requesting the tag is responsible for maintaining the entry in the high side database. For example, Figure 6 shows an example of a partial database containing information about each registered information resource. Note that not all attributes are shown for brevity.

Tag	Owner	Producer	Age	Criticality	Contains	SA_LABEL
7FD3BA30	AFIOC	33 rd IOS	Daily	Very High	23A9D3D7, DD3100AC	TS/SCI/HCS
B723AA29	67 th NWW	GREEN TEAM	01 OCT 2007	High	<NULL>	Secret/BELL
23A9D3D7	NASIC	SMAI	Daily	Very High	<NULL>	TS/SCI/TK
DD3100AC	NSA	GROUP 4	Weekly	High	<NULL>	TS/SCI

Figure 6: CIMIA Abbreviated Example High Side Database

Before the tags are inserted into an information stream, they are encrypted using symmetric key encryption. The tag encryption key is automatically changed daily so even if the tags are intercepted they can not be used to infer anything about the source. This is accomplished by using a pseudorandom number generator which is seeded monthly basis using information acquired from the central authority. This reduces the likelihood of an adversary from gaining additional information if they were able to capture tags from different locations. The encrypted tags are “intelligently” inserted into the information stream at the source upon the first request from a requestor and then periodically thereafter based upon a predefined policy. As a result, the tagging of the data incurs a very low overhead considering the benefit derived. Encrypted tags can be safely ignored by non-participating information sinks (consumers). By storing all sensitive data about the information resource on a separate higher security network, information can only be derived from the tag by authorized entities.

The use of encrypted information resource tags provides multiple benefits. The tags can be tracked by any intermediate infrastructure elements for critical infrastructure identification or traffic prioritization purposes; tags can be recorded during exercises and operations to develop statistical templates of mission information dependencies; and most importantly provide the

ability to automate the linking of information sources and information sinks making dynamic mapping of changes possible.

We are currently investigating various ways (e.g., in-band, out-of-band) that the encrypted tags would be inserted into information streams. It is desired that the mechanism be transparent so that if an information resource is relocated, the encrypted tag will be transported with the relocated information. This provides the capability to identify copies of information resources provided by multiple sources and will maintain the ability for the central authority to identify all downstream consumers of the resource is compromised.

6.3 Information Source (Provider) Requirements

As the information source (provider) supplies information resources to information sinks (consumers), the source will record the access in a lightweight database stored locally on the sourcing system. Each transaction is not explicitly logged, but instead summary statistics are collected on each information requestor. The lightweight database enables the source to identify new information accesses which require a tag to be inserted and provides a historical record of accesses. Periodically, the contents of the sourcing system lightweight database will be transferred to a local organizational database where it is subsequently forwarded through a secure mechanism to the central authority. The central authority now has the information that it needs to enforce valuation accountability of information consumers. Specifically, the central authority will require each information consuming organization to forward its critical asset profile which identifies the mission processes supported by the accessed information resource and how the consuming organization values the resource. This enables the central authority to identify all consumers of a given information resource and to compute an aggregate valuation for the information resource.

6.4 Information Sink (Consumer) Requirements

As the information sink (consumer) requests information resources from information sources (provider), the sink will record the access in a lightweight database stored locally on the sinking system. Information consumers will be required to assign one or more mission processes to the information access and to assign a value to the information access. A variety of approaches could be used to collect this information ranging from asking the information consumer the instant they access the resource, to asking the information consumer at the end of their shift. In a military setting, it is likely that the later would be preferred. In this case, at the end of each shift the consumer is required to proceed through a question and answer session where they link each information resource they accessed to one or more mission processes identified in a pull down list. In addition, the information consumer is will value the importance of the information resource. While initially the effort required by each consumer might be substantial, over time the CIMIA process would “learn” which information resources support which mission processes and how critical the dependency is. Periodically, the contents of the sinking system lightweight database will be transferred to a secure organizational database where it is subsequently forwarded through a secure mechanism to the central authority. The organizational database is responsible for the aggregation of information dependency and valuation information and serves as the Critical Cyber Asset Profile (C-CAP) for the organization.

Since the organizational database contains information about all of the organizations information dependencies and their valuation, this information must be highly protected. Exploitation of this information by an adversary would provide a targeting map of the organization. In our initial conception of the process, the information will have to be stored on a separate, higher classification system in a network separate from that which is being operationally used.

While this methodology has the potential to be bothersome to personnel when first implemented, new implementations could be primed with information gained from a manual assessment to reduce the effort required. A dependency report would be generated on a regular basis and reviewed by consumers to validate the accuracy of their assessments. Organizational units could implement a peer review to insure operators are properly completing the assessment. While this will no doubt require a cultural change and buy-in from the organizational leadership, we believe the benefits provided will far outweigh the cost in effort from personnel.

The information contained in the local organizational database will be used to drive a situational awareness display to the commander. Although not discussed in detail in this paper, CIMIA will allow a commander to visualize worst case, best case, and average case impacts due to a cyber incident; will allow for the visualization of uncertainty to show the confidence of the mission impact estimation; and will account for temporal aspects of mission processes to identify future potential impacts when a cyber asset that will be needed in the near future is currently unavailable or has been compromised.

It is further contemplated that the organization will create temporal mission profiles that reflect how their information dependencies change over time. These temporal mission profiles, when convolved with the current status information, provide the ability to recognize future information dependencies which may negatively impact the organizational mission.

6.5 Central Authority Process

The central authority places a key role in the CIMIA process. It serves to link information resource requests collected from information sources with the corresponding Critical Cyber Asset Profiles (C-CAPs). Based upon the information transmitted in the C-CAPs, the central authority can identify all information dependencies and their valuation and calculate an aggregate enterprise wide valuation for each information resource. It provides the capability for the central authority to immediately notify downstream information consumers when an incident occurs. Consuming organizations will periodically download an encrypted status message from the central authority on the low side system. The encrypted status message includes a list of organizations that may be affected by current cyber incidents. This pull-type architecture does not provide an adversary monitoring the network with knowledge that might be apparent with a push-type of architecture. Each organization will then be responsible for accessing the central authority on the high-side system to identify which of their information dependencies are adversely affected. This information is used by the organization in conjunction with their local C-CAP to determine current and potential impacts resulting from cyber incidents to drive the

CIMIA situational awareness display providing organizations with a near real-time predictive mission impact assessment from the moment a cyber incident occurs.

7 Conclusions

Despite the fact that the need for effective cyber damage assessment was recognized more than a decade ago, little progress has been made to attain this objective. The explosive growth of cyber attacks and the dependency on cyberspace to conduct military operations has awakened commanders to the shortcomings of existing damage assessment capabilities. While taking an infrastructure-based approach to cyber security is “easier,” it does not provide the information needed to produce accurate and timely damage or mission impact assessment. Information should be viewed as an asset and we should focus our efforts on developing technology assisted information asset identification, valuation, tracking, documentation, and reporting capabilities.

In this paper, we proposed a scalable, self-documenting, distributed information asset tracking methodology that provides the capability to identify information dependencies, does not incur significant overhead, and prevents an adversary from gaining knowledge from intercepted communications. We believe such a methodology will significantly enhance the timeliness and accuracy of cyber damage assessment; enable near real-time mission impact assessment; meet the joint requirements on reporting cyber damage assessment; and enable predictive situational awareness to provide commanders with dominate battlespace knowledge in cyberspace.

8 Disclaimer

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

References

- [1] Denning, D., “Information Warfare and Security,” Upper Saddle River, NJ, Pearson, 1999.
- [2] Joint Chiefs of Staff, “Joint Publication 3-13: Information Operations,” United States Department of Defense, 13 February 2006.
- [3] National Defense University Press, “Dominant Battlespace Knowledge,” M. C. Libicki and S. E. Johnson (Ed), October, 1995.
- [4] Grimaila, M.R. & L.W. Fortson, “Towards an Information Asset-Based Defensive Cyber Damage Assessment Process,” Computational Intelligence in Security and Defense Applications (CISDA 2007), 206-212, April 1-5, 2007.
- [5] Fortson, L.W. & M.R. Grimaila, “Development of a Cyber Damage Assessment Framework,” International Conference on Information iWarfare and Security (ICIW 2007), March 8-9, 2007.
- [6] Fortson, L.W., “Towards the Development of a Defensive Cyber Damage and Mission Impact Methodology,” Master's thesis, Air Force Institute of Technology, Department of Systems and Engineering Management, March 2007.

- [7] Pipkin, D.L., "Information Security Protecting the Global Enterprise," Hewlett-Packard Company, 2000.
- [8] Diehl, J.G. & C.E. Sloan, "Battle damage assessment: the ground truth," Joint Force Quarterly, 2004.
- [9] Owens, Adm. W., "Lifting the Fog of War," New York: Farrar, Straus and Giroux, 2000.
- [10] United States General Accounting Office, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," United States General Accounting Office Chapter Report, 22 May 1996.
- [11] Theim, L., "A Study to Determine Damage Assessment Methods or Models on Air Force Networks," Air Force Institute of Technology, Wright Patterson Air Force Base, OH, 2005.
- [12] Horony, Mark D. "Information system incidents: the development of a damage assessment model." Masters Thesis, Wright-Patterson AFB OH: Air Force Institute of Technology (AFIT), 1999.
- [13] Lala, C. & B. Panda, B. "Evaluating damage from cyber attacks." IEEE Transactions on Systems, Man and Cybernetics 31(4): 300-310, 2000.
- [14] Arvidsson, J. "Taxonomy of the Computer Security Incident Related Terminology," TERENA Incident Taxonomy and Description Working Group, 2007, http://www.terena.org/activities/tf-csirt/iodef/docs/i-taxonomy_terms.html
- [15] Oxford, "The Oxford Reference Dictionary," Oxford University Press, 1986.
- [16] Endsley, M.R., "Toward a Theory of Situation Awareness in Dynamic Systems," Human Factors Journal, 37(1), 32-64, March 1995.
- [17] Taddaa, G., J. Salerno, D. Boulware, M. Hinman, & S. Gorton, "Realizing Situation Awareness in a Cyber Environment," Proceedings of SPIE; Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications, vol. 6242, 2006.
- [18] Finne, T. "Information systems risk management: Key concepts and business processes," Computers & Security, 19, 3 (2000), 234-242.
- [19] NIST SP 800-30 (2002), "Risk Management for Information Technology Systems," National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 (2002).
- [20] Mercuri, R. T., "Analyzing Security Costs," CACM, 46, 6. June 2003, 15-18.
- [21] Gordon, L.A. and Loeb, M.P., "The Economics of Information Security Investment," ACM Transactions on Information and System Security, 5, 4. November 2002, 438-457.
- [22] DIACAP. "DoD Information Assurance Certification and Accreditation Process (DIACAP) and DoD Information Technology Security Certification & Accreditation Process (DITSCAP)," Information Assurance Support Environment, DISA, 2007, <http://iase.disa.mil/ditscap/>
- [23] DoD 8510.01, "Department of Defense Instruction 8510.01 - DoD Information Assurance Certification and Accreditation Process (DIACAP)," ASD(NII)/DoD CIO, November 28, 2007.
- [24] Soo Hoo, K.J., "How Much Is Enough? A Risk Management Approach to Computer Security," Consortium for Research on Information Security and Policy (CRISP), Stanford University, 2000.
- [25] Davenport, T.H. & L. Prusack, "Working Knowledge: How Organizations Manage What They Know," Boston, Harvard Business School Press, 1998.

- [26] Petrocelli, T.D., "Data Protection and Information Lifecycle Management," Upper Saddle River, New Jersey, Pearson Education, Inc., 2005.
- [27] Stevens, J.F., "Information Asset Profiling," Pittsburgh, PA, Carnegie Mellon University, 2005.
- [28] Drucker, P.E., "The Post Capitalistic Executive" in P.E. Drucker (ed.) Management in a Time of Great Change New York: Penguin, 1995.
- [29] Alberts, C.J., A. Dorofee, J. Stevens, & C. Wooky, "Introduction to the OCTAVE approach," Pittsburgh, PA, Carnegie Mellon University, 2003.
- [30] Alberts, C.J. & A. Dorofee, "Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments," Networked Systems Survivability Program, Carnegie Mellon University, 2005.
- [31] Van Alstyne, M.V., "A proposal for valuing information and instrumental goods," Proceeding of the 20th International Conference on Information Systems Charlotte, North Carolina, United States Association for Information Systems, 1999.
- [32] EO13292, "Executive Order 13292 - Further Amendment to Executive Order 12958," as Amended, Classified National Security Information, 2003.
- [33] AFI 33-138. Air Force Instruction (AFI) 33-138: Enterprise Network Operations Notification and Tracking. Department of the Air Force. SAF/XCIF: (2004), Ch. 3 and 5.
- [34] AFDD 2-5. Air Force Doctrine Document (AFDD) 2-5 Information Operations. Department of the Air Force, HQ AFDC/DR, (2005).

Author Biographies

Michael R. Grimaila is an associate professor of Information Resource Management in the Department of Systems and Engineering Management and member of the Center for Cyberspace Research at the Air Force Institute of Technology (AFIT). Dr. Grimaila received a BS and MS degree in Electrical Engineering, and a Ph.D. in Computer Engineering at Texas A&M University. He teaches and conducts research in the areas of information assurance, information warfare, and information operations. He holds the CISM, CISSP, and NSA IAM/IEM certifications. EMAIL: michael.grimaila@afit.edu

Robert F. Mills is an assistant professor of Electrical Engineering in the Department of Electrical and Computer Engineering and member of the Center for Cyberspace Research at the Air Force Institute of Technology (AFIT). Dr. Mills received a BS degree in Electrical Engineering from Montana State University, an MS degree in Electrical Engineering from AFIT, and a PhD in Electrical Engineering from the University of Kansas. He teaches and conducts research in the areas of communications systems, signal detection and exploitation, network security/management, and cyber operations and warfare.

Capt. Larry W. Fortson, USAF is Chief of the Information Operations and Cyberspace Research group of the Information Operations & Special Programs Division of the Air Force Research Laboratory (AFRL/RHX). EMAIL: larry.fortson@wpafb.af.mil